(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 770 067**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **97 12973**

(51) Int Cl[6] : **H 04 L 9/12**, G 06 F 12/14 // G 07 F 7/10

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 16.10.97.

(30) **Priorité** :

(43) **Date de mise à la disposition du public de la demande** : 23.04.99 Bulletin 99/16.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *FRANCE TELECOM SOCIETE ANONYME* — FR.

(72) **Inventeur(s)** : MOUNIER JEAN PIERRE.

(73) **Titulaire(s)** :

(74) **Mandataire(s)** : SOCIETE DE PROTECTION DES INVENTIONS.

(54) PROCEDE D'ACCES A UNE APPLICATION.

(57) La présente invention concerne un procédé d'accès à une application dans lequel on utilise un code confidentiel. Dans ce procédé on prévoit en accord avec l'usager du code, un algorithme d'évolution de ce code en partant d'un code de base.

FR 2 770 067 - A1

PROCEDE D'ACCES A UNE APPLICATION

DESCRIPTION

Domaine technique

La présente invention concerne un procédé d'accès à une application, dans lequel on utilise un code confidentiel.

Etat de la technique antérieur

L'accès à de nombreuse applications est protégé par l'utilisation d'un code confidentiel. Ce code peut être modifié par l'intéressé, pour un accès à son calculateur personnel par exemple, ou par les responsables de ces applications.

Si quelqu'un prend connaissance du code personnel donnant accès à une application (vol d'une carte avec le code par exemple) il lui est aisé de s'introduire frauduleusement dans l'application. Il lui est aussi possible de faire des essais multiples de codes d'accès. Pour résoudre ce problème il est possible de changer un code et de le mémoriser, mais cette procédure est lourde.

L'invention a pour objet de changer automatiquement le code, autant de fois qu'on le veut, en possédant un moyen simple de s'en souvenir.

Exposé de l'invention

La présente invention concerne un procédé d'accès à une application dans lequel on utilise un code confidentiel, caractérisé en ce qu'on prévoit, en

accord avec l'usager du code, un algorithme d'évolution du code en partant d'un code de base.

Avantageusement l'algorithme est pris parmi les algorithmes suivants :

- algorithmes utilisant l'heure ;
- algorithmes utilisant le jour de la semaine ;
- algorithmes utilisant la semaine ;
- algorithmes utilisant le jour du mois ;
- algorithmes utilisant le mois ;
- algorithmes utilisant l'année ;
- algorithmes utilisant une table particulière ;
- algorithmes utilisant plusieurs paramètres, qui sont la concaténation de plusieurs algorithmes.

On peut de plus utiliser un algorithme de secours.

Avantageusement la modification d'algorithme peut être faite en ligne ou via un mécanisme de changement automatique connu à la fois par le propriétaire du code et le serveur associé à l'application que l'on veut utiliser.

Le mécanisme peut être introduit dans toute application qui demande un code d'accès.

Toutes les applications informatiques peuvent utiliser ce type de codes pour se protéger. On peut, par exemple, s'en servir pour contrôler un code d'accès et autoriser ou non un accès à certaines heures.

Dans un exemple de réalisation l'usager utilise une carte. On peut alors avoir les étapes suivantes :

- à l'achat d'une carte, l'usager choisit, dans un catalogue, l'algorithme qu'il désire et donne

les paramètres qui seront utilisés par cet algorithme ; le vendeur de la carte saisit le numéro de l'algorithme et les paramètres ; le serveur remplit la table correspondant au fichier de l'usager ;

- quand l'usager introduit sa carte, les caractéristiques de la carte et du terminal permettent de :
  - identifier le porteur de la carte et de trouver son fichier,
  - savoir s'il a accès à l'application et s'il peut l'utiliser actuellement,
  - connaître sa table de code ;
- l'usager frappe le code correspondant aux paramètres qu'il a lui-même définis.

Brève description des figures

- La figure illustre le contexte d'utilisation du procédé de l'invention.

Exposé détaillé de modes de réalisation

L'invention consiste à prévoir, en accord avec l'usager du code, un algorithme d'évolution de celui-ci en partant d'un code de base, cette évolution pouvant avoir lieu n'importe quand, avec n'importe quelle fréquence.

Dans un premier exemple : sur le code JPM on décide de greffer l'heure et le jour sous la forme J14P11M où 14 représente l'heure (2 pm) et onze mois. Au pire il peut y avoir une incertitude à la frontière de l'heure mais on peut présenter deux codes successivement.

Dans un second et un troisième exemples : au code CESTMOI on peut ajouter le jour de la semaine codé ou éliminer une lettre :

le dimanche	CESTMOIREPOS	ou	ESTMOI
le lundi	CESTMOIDEBUT	ou	CSTMOI
le mardi	CESTMOIMARS	ou	CETMOI
le mercredi	CESTMOIECOL	ou	CESMOI
le jeudi	CESTMOIJEUD	ou	CESTOI
le vendredi	CESTMOIFINI	ou	CESTMI
la samedi	CESTMOIWEWE	ou	CESTMO

Seule l'imagination peut limiter les possibilités de l'invention. On peut donner un exemple complet de fonctionnement d'un serveur sur des algorithmes convenus avec l'usager.

EXEMPLE DE GESTION DE CES CODES

Dans un exemple de réalisation, illustré sur la figure, à l'achat d'une carte, l'usager choisit, dans un catalogue, l'algorithme qu'il désire et donne les paramètres qui seront utilisés par cet algorithme.

Le vendeur saisit le numéro de l'algorithme et les paramètres au nombre maximum de, par exemple, quatre.

Le serveur remplit la table correspondant au fichier de l'usager.

Quand l'usager introduit sa carte, les caractéristiques de la carte et du terminal permettent de :

- identifier le porteur de la carte et de trouver son fichier ;

- savoir s'il a accès à l'application et s'il peut l'utiliser actuellement (par exemple code bancaire approvisionné) ;

- connaître sa table de code.

L'usager frappe le code correspondant aux paramètres qu'il a lui même définis.

L'usager peut redéfinir les caractéristiques de ce code évolutif, en allant voir la personne qui a accès à l'application. L'usager peut également changer son algorithme en ligne.

Par exemple les algorithmes choisis et les paramètres à utiliser sont donnés directement en ligne par le responsable de l'introduction de la nouvelle carte. Il suffit de remplir, dans la table Code_nom_de_l'usager, le code de base, le numéro d'algorithme et les paramètres.

Pour plus de facilités, les algorithmes peuvent être classés comme suit dans le catalogue :

- algorithmes utilisant l'heure (00 à 11 am/pm ou 00 à 23) ;

- algorithmes utilisant le jour de la semaine (Lu, Ma, ..., Di) ;

- algorithmes utilisant la semaine (numéro de la semaine) ;

- algorithmes utilisant le jour du mois (01,...,31) ;

- algorithmes utilisant le mois (numéro du mois) ;

- algorithmes utilisant l'année (97 ou 1997) ;

- algorithmes utilisant une table particulière ;

- algorithmes utilisant plusieurs paramètres, qui sont la concaténation de plusieurs algorithmes.

Quand on parle d'heure, de jour, ..., d'année, il s'agit du contenu du champ correspondant au numéro de l'heure, du jour, ..., de l'année. En fait l'algorithme peut ignorer que ce paramètre est une heure, un jour, ..., une année. Le contenu des tables indique où il faut prendre la valeur de ce paramètre. Les algorithmes deviennent, dans le serveur :

- l'algorithme 100 utilise le paramètre 1 ajouté en tête du code de base ;
- l'algorithme 101 utilise le paramètre 1 ajouté après le 1er caractère du code de base ;
- l'algorithme 102 utilise le paramètre 1 ajouté après le 2ème caractère du code de base ;
- l'algorithme 103 utilise le paramètre 1 ajouté après le 3ème caractère du code de base ;
- etc...
- l'algorithme 10x utilise le paramètre 1 ajouté à la fin du code de base ;
- l'algorithme 200 utilise le paramètre 2 ajouté en tête du code de base ;
- etc...
- l'algorithme y0x utilise le paramètre y ajouté à la fin du code de base.

Pour les exemples 1 et 3 on a l'algorithme 000 : le paramètre est égal à i ; on enlève le ième caractère.

La Table_Code_nom_de_l'usager permet de retrouver le contenu du paramètre. Elle a la forme suivante :

Code de base	Code de base	Code de secours
Algorithmes	Algorithme de base	Algorithme de secours
Paramètre 1	Type	Table
Paramètre 2	Type	Table
Paramètre n	Type	Table

où Type=l'heure, le jour, la semaine, le mois, l'année ou la table définie dans Table.

On donne ici la possibilité d'utiliser un code et un algorithme de secours. Cela permet de varier les possibilités mais complique la gestion des tables. Le choix du code peut être fait en ligne.

Dans le premier exemple :

• Vu par l'usager

Il est 14 heures et on est en novembre, son code personnel (de base) est JPM. Il tape J14P11M.

• Vu par le serveur

La carte introduite dans le publiphone 78456 indique au serveur que Monsieur Jean-Pierre Mounier veut accéder à un service de France Telecom qui exige un code sécurisé.

Dans le fichier Jean_Pierre_Mounier il y a la table : Code_Jean_Pierre_Mounier :

Code de base	JPM	Pas de code de secours
Algorithmes	101-102	Pas d'algorithme de secours
Paramètre 1	Type = heure	
Paramètre 2	Type = mois	
	FIN	

L'algorithme à utiliser est 101-202 (deux paramètres).

Algorithme 101 :
Ajouter P1 en Code_de_base [caractère_1+1]
commentaires : car1, P1, car2, car3, ..., carn
Algorithme 202 :
Ajouter P2 en Code_de_base [caractère_2+1]
commentaire : car1, P1, car2, P2, car3, ..., carn

Code_de_base = JPM
P1 = l'heure = 14
P2 = le mois = 11

Code attendu = J14P11M, c'est bien celui qui a été frappé.

Dans le second exemple :

• Vu par l'usager

On est vendredi, le semaine est finie, le code de base est CESTMOI. Je tape CESTMOIFINI.

• Vu par le serveur

La table Code_Jean_Pierre_Mounier a la forme suivante :

Code de base	JPM	Pas de code de secours
Algorithmes	109	Pas d'algorithme de secours
Paramètre 1	Type = jour de semaine	Table = JPM1
	FIN	

L'algorithme 109 utilise le paramètre 1 ajouté à la fin du code de base.

La table JPM1 a la forme suivante :

Dimanche	REPOS
Lundi	DEBUT
Mardi	MARS
Mercredi	ECOL
Jeudi	JEUD
Vendredi	FINI
Samedi	WEWE

On est le 6 juin 1997, c'est un vendredi. La table JPM1 donne FINI pour vendredi. Le code de base est CESTMOI. L'algorithme 109 dit d'ajouter le contenu de la table JPM1 au code de base. Le code attendu est CESTMOIFINI.

Dans le troisième exemple :

- Vu par l'usager

Cette méthode demande plus de réflexion de la part de l'usager. On est le lundi 9 juin. C'est un lundi deuxième jour de la semaine. Donc l'usager doit enlever la deuxième lettre de son code qui est CESTMOI. Donc il enlève le E et il obtient CSTMOI.

On voit ici que l'usager a intérêt à utiliser un algorithme intuitif et simple.

- Vu par le serveur

La table Code_Jean_Pierre_Mounier a la forme suivante :

Code de base	JPM	Pas de code de secours
Algorithmes	000	Pas d'algorithme de secours
Paramètre 1	Type = jour	JPM1

	de semaine	
	FIN	

La table JPM1 a la forme suivante :

Dimanche	1
Lundi	2
Mardi	3
Mercredi	4
Jeudi	5
Vendredi	6
Samedi	7

On est le 9 juin 1997, c'est un lundi. La table JPM1 donne 2 pour lundi. Le code de base est CESTMOI. L'algorithme 000 dit d'enlever le ième caractère au code de base. Ici i est égal à 2. Le code attendu est CESTMOI moins la deuxième lettre, c'est-à-dire CSTMOI.

On peut aller du plus simple : l'usager donne le jour de la semaine, au plus compliqué du style : le code de base est Jean-Pierre Mounier, l'usager le transforme en :

1. Il enlève la lettre correspondant au jour de la semaine.
2. Il ajoute le numéro de la semaine après Jean.
3. Il ajoute le numéro du mois après Pierre.
4. Il ajoute en fin de code l'heure.

Ce qui donne : on est le 9 juin à 15h30 et c'est un lundi :

1. Il enlève la lettre correspondant au jour de la semaine (2) ⇒ JanPierreMounier.
2. Il ajoute le numéro de la semaine après Jean (24) ⇒ Jan24PierreMounier.
3. Il ajoute le numéro du mois après Pierre (06) ⇒ Jan24Pierre06Mounier.
4. Il ajoute en fin de code l'heure (15) ⇒ Jan24Pierre06Mounier15.

Ce code est inutilisable pour un tiers et le serveur s'y retrouve facilement.

REVENDICATIONS

1. Procédé d'accès à une application comprenant une étape de mise en place, par le responsable de cette application, d'un code d'accès à celle-ci, et une étape d'introduction, par un usager d'un système informatique, de ce code permettant à celui-ci d'utiliser cette application, caractérisé en ce que dans la première étape le responsable de l'application choisit une modification automatique du code suivant un algorithme d'évolution en partant d'un code de base.

2. Procédé selon la revendication 1, dans lequel on a les étapes suivantes :

- à l'achat d'une carte, l'usager choisit, dans un catalogue, l'algorithme qu'il désire et donne les paramètres qui seront utilisés par cet algorithme ; le vendeur de la carte saisit le numéro de l'algorithme et les paramètres ; un serveur remplit la table correspondant au fichier de l'usager ;
- quand l'usager introduit sa carte les caractéristiques de la carte et du terminal permettent de :
  - identifier le porteur de la carte et de trouver son fichier,
  - savoir s'il a accès à l'application et s'il peut l'utiliser actuellement,
  - connaître sa table de code ;
- l'usager frappe le code correspondant aux paramètres qu'il a lui-même définis.

3. Procédé selon la revendication 1, caractérisé l'algorithme est pris parmi les algorithmes suivants :

- algorithmes utilisant l'heure ;

- algorithmes utilisant le jour de la semaine ;
- algorithmes utilisant la semaine ;
- algorithmes utilisant le jour du mois ;
- algorithmes utilisant le mois ;
- algorithmes utilisant l'année ;
- algorithmes utilisant une table particulière ;
- algorithmes utilisant plusieurs paramètres, qui sont la concaténation de plusieurs algorithmes.

4. Procédé selon la revendication 1, dans lequel on utilise un algorithme de secours.

5. Procédé selon la revendication 1, dans lequel le choix de l'algorithme est fait en ligne.

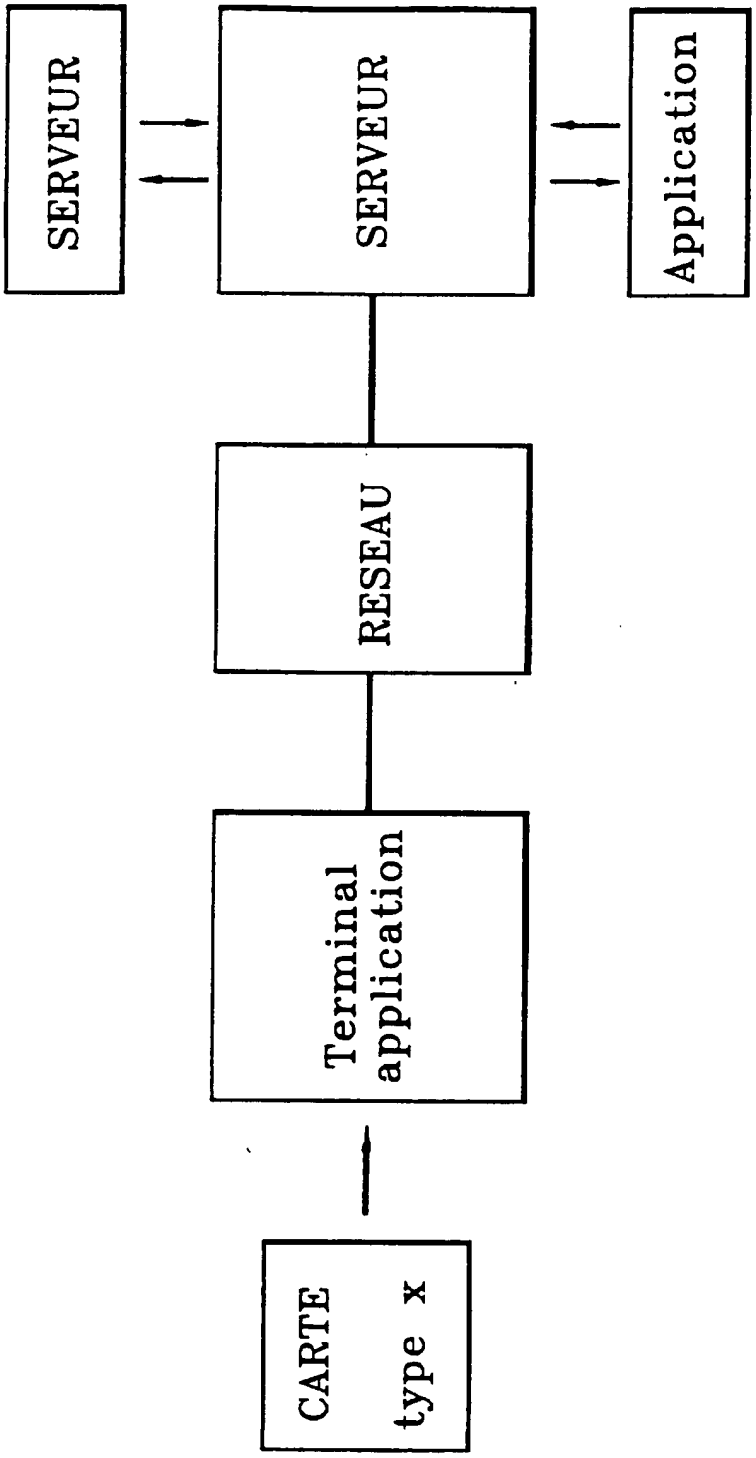
SERVEUR
SERVEUR
Application
RESEAU
Terminal application
CARTE type x

FIG. 1

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2770067
N° d'enregistrement national

FA 551482
FR 9712973

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée	
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
Y	EP 0 561 685 A (FUJITSU LTD) 22 septembre 1993 * abrégé; figures 1,2 * * colonne 3, ligne 32 - colonne 4, ligne 46 * ---	1,2,5	
Y	US 5 163 097 A (PEGG TINA C) 10 novembre 1992 * le document en entier * ---	1,2,5	
A	WO 87 03977 A (GORDIAN SYSTEMS INC) 2 juillet 1987 * le document en entier * ---	1,3	
A	US 5 509 070 A (SCHULL JONATHAN) 16 avril 1996 * le document en entier * ---	1,3	
A	WO 96 34328 A (WEISZ HERMAN ;LO PIANO ORNELLA (IT)) 31 octobre 1996 * abrégé * ---	1,3	
A	WO 97 36221 A (ROLM SYSTEMS) 2 octobre 1997 * page 2, alinéa 2 - page 3, alinéa 1 * -----	1,4	DOMAINES TECHNIQUES RECHERCHES (Int.CL.6) G06F

1

Date d'achèvement de la recherche	Examinateur
10 juillet 1998	Powell, D

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

.....

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)